HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: PCB EDTB 06-03 Internet Phishing
SPONSOR(S): Economic Development, Trade & Banking Committee
TIED BILLS: **IDEN./SIM. BILLS:**

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR
Orig. Comm.: Economic Development, Trade & Banking Committee		Olmedillo	Carlson
1)			
2)			
3)			
4)			
5)			

SUMMARY ANALYSIS

This bill creates the "Anti-Phishing Act of 2006" and will prohibit the acquisition of personal identifying information through the use of a website or e-mail with the intent to possess or use such information fraudulently.

The bill creates a civil cause of action for Internet access providers and web page or trademark owners harmed by a violation as well as the Attorney General.

The bill provides these plaintiffs with the power to seek injunctive relief and damages in the greater amount of the actual damages arising from the violation, or $100,000, for each violation of the same nature. A court may increase damages to three times the actual damages sustained if violations constitute a pattern. The bill does not preclude the award of damages otherwise available under federal or state law.

The bill provides for an award of attorney's fees and costs to a prevailing plaintiff.

The bill also makes a violation a prohibited act under the Florida Deceptive and Unfair Trade Practices Act.

The bill provides for an effective date of October 1, 2006.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. HOUSE PRINCIPLES ANALYSIS:

Safeguard individual liberty: The bill should deter identity theft in Florida, protecting Florida citizens.

Promote personal responsibility: The bill increases personal accountability for unlawful actions and injurious behavior.

Limited Government: The bill creates a new civil cause of action designed to deter and punish illegal activity.

B. EFFECT OF PROPOSED CHANGES:

Present Situation

Identity theft is a substantial problem in the United States and "phishing" represents the cutting edge of this devious practice.

"Phishing" refers to obtaining personal identifying information from individuals via the Internet with the intent to possess or use such information fraudulently. Typically, a person attempting to obtain information sends an e-mail that appears to come from a bank or other trusted business requesting an individual to verify their account by typing personal identifying information, such as credit card information, social security numbers, account usernames, passwords, etc. Another method is to use a phony web site to trick citizens into forfeiting sensitive personal information.

The Federal Trade Commission (FTC) reported that 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in 2003 alone.[1] According to the FTC, last year's identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses.[2]

Moreover, according to the Anti-Phishing Working Group, the volume of fraudulent phishing e-mail is growing at a rate in excess of 30 percent each month.[3]

Florida Deceptive and Unfair Trade Practices Act

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA), Chapter 501 part II, F.S., makes unlawful unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce. "Trade or commerce," which includes the conduct of any trade or commerce, however denominated, including any nonprofit or not-for-profit person or activity, is defined as the advertising, soliciting, providing, offering or distributing, whether by sale, rental, or rental, or otherwise of any good or service or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated.[4]

---

[1] See article issued by Federal Trade Commission, dated September 3, 2003 "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers". See also http://www.ftc.gov/opa/2003/idtheft.htm.

[2] Id.

[3] The Anti-Phishing Working Group (APWG) is a global pan-industrial and law enforcement association that focuses on eliminating fraud and identity theft that results from phishing and e-mail spoofing of all types.

[4] Section 501.203(8), F.S.

The enforcing authority of the FDUTPA is the local state attorney for violations within a single judicial circuit or the Department of Legal Affairs if the violation occurs in or affects more than one judicial circuit or, in cases affecting a single judicial circuit, when the office of the state attorney defers to the department in writing, or fails to act upon a violation within 90 days after a written complaint has been filed with the state attorney.[5] The act provides for cease and desist orders, remedies by the enforcing authority, civil penalties, and receipt by the prevailing party of attorney's fees and costs in civil litigation.[6]

A willful violation of FUDTPA subjects the violator to a civil penalty of not more than $10,000 for each violation.[7] In any civil litigation initiated by the enforcing authority, the court may award to the prevailing party reasonable attorney's fees and costs if the court finds that there was a complete absence of a justiciable issue of either law or fact raised by the losing party or if the court finds bad faith on the part of the losing party.[8]

An individual harmed by a violation of the FUDTPA may, without regard to any other remedy or relief to which the person is entitled, bring an action to obtain a declaratory judgment that an act or practice violates the FUDTPA and to enjoin a person who has violated, is violating, or is otherwise likely to violate the act.[9] In such an action, the person may recover actual damages, plus attorney's fees and court costs.[10]

Anti-Phishing Bills in Congress

The Subcommittee on Crime, Terrorism, and Homeland Security of the U.S. House of Representatives is currently reviewing H.R. 1099, which criminalizes internet scams involving the fraudulent obtaining of information, commonly known as "phishing".[11]

H.R. 1099 bill imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in an activity constituting fraud or identity theft under Federal or State law: (1) creates or procures the creation of a website or domain name that represents itself as a legitimate online business without the authority or approval of the registered owner of such business; and (2) uses that website or domain name to solicit means of identification from any person.

In addition, H.R. 1099 imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in activity constituting fraud or identity theft under Federal or State law sends an electronic mail message that: (1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet location tool referring or linking users to an online location on the World Wide Web that falsely purports to belong to or be associated with a legitimate online business; and (3) solicits means of identification from the recipient.

Effect of Proposed Changes

Name

Creates the "Anti-Phishing Act of 2006".

[5] Section 501.203(2), F.S.
[6] Section 501.208(1), F.S.
[7] Section 501.619, F.S.
[8] Section 501.621, F.S.
[9] Section 501.211(1), F.S.
[10] Section 501.211(2), F.S.
[11] The Senate companion, S.472 is before the Judiciary Committee.

Prohibited Acts

This bill prohibits obtaining identifying information from individuals through certain means via the Internet with the intent to possess or use such information fraudulently. The bill prohibits:

- Creating a web page or Internet domain name representing a legitimate online business without the business owner's authorization; and
- Using that web page, a link to the web page, or another site on the Internet to induce, request, or solicit another person to provide identifying information for a purpose that the other person believes is legitimate.

The bill also prohibits sending or causing to be sent an e-mail to a resident of this state that:

- Falsely represents itself as being sent from a legitimate business;
- Refers or links the recipient to a falsely represented web site; and
- Directly or indirectly solicits from the recipient identifying information for a purpose that the recipient believed to be legitimate.

The bill creates definitions for use in interpreting and implementing the protections of this part, as follows:

- "**Electronic mail message**" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.[12]

- "**Electronic mail address**" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.[13]

- "**Identifying information**" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

  1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

  2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

  3. Unique electronic identification number, address, or routing code;

  4. Medical records;
  5. Telecommunication identifying information or access device; or

  6. Other number or information that can be used to access a person's financial resources.[14]

[12] s. 668.602(7), F.S.
[13] s. 668.602(6), F.S.
[14] s. 817.568(1)(f), F.S.

- "**Internet domain name**" means a globally unique, hierarchical reference to an Internet host or service, which is assigned through centralized Internet naming authorities and which is comprised of a series of character strings separated by periods, with the right-most string specifying the top of the hierarchy.[15]

- "**Web page**" means a location that has a single uniform resource locator (URL) with respect to the world wide web or another location that can be accessed on the Internet.

Remedies

The bill gives standing to bring a civil action under this part to:

- An Internet access provider providing services to the public who was harmed by a violation under this bill;
- An owner of a web page or trademark who was harmed by a violation under this bill; or
- The Attorney General.

A person bringing an action may seek injunctive relief to halt a violation under this bill, recover damages in the greater amount of the actual damages arising from the violation, or $100,000 for each violation of the same nature, or seek both injunctive relief and recover damages. Violations are considered of the same nature if they consisted of the same action or course of conduct regardless of how many times the act occurred. A court may increase damages to three times the actual damages sustained if violations constitute a pattern or practice.

The bill also provides for an award of attorney's fees and costs to a prevailing plaintiff.

The bill does not preclude the award of damages otherwise available for the same conduct pursuant to federal or state law. Moreover, this bill renders a prohibited act under this part a Florida Deceptive and Unfair Trade Practice under ch. 501, F.S.

Exemption

The bill exempts from liability a telecommunication provider's or an Internet service provider's good faith transmission or intermediate temporary storing of identifying information.

C. SECTION DIRECTORY:

Section 1: Creates s.668.6076, F.S. to provide a title; s.668.6077, F.S., to provide definitions; s.668.6078, F.S. to provide prohibited acts; s.668.6079, F.S. to provide remedies and standing; and s.668.6080, F.S. to provide an exemption.

Section 2: Provides an effective date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   See Fiscal Comments.

2. Expenditures:

[15] s. 668.602(10), F.S.

See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

This bill may lessen the frequency of identify theft and the costs associated with such theft, to the benefit of Florida citizens and businesses.

D. FISCAL COMMENTS:

The Attorney General could bring an action to recover damages in the greater amount of the actual damages arising from the violation, or $100,000 for each violation of the same nature, or seek both injunctive relief and recover damages. A court could increase damages to three times the actual damages sustained if violations constituted a pattern. The revenue derived from these actions is indeterminate.

The bill grants the Attorney General authority to enforce violations under this bill. Therefore, the Attorney General will incur costs in order to prosecute persons that violate this bill. The costs, however, are indeterminate.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The bill does not require a municipality or county to expend funds or to take any action requiring the expenditure of funds. The bill does not reduce the authority that municipalities or counties have to raise revenues in the aggregate. The bill does not reduce the percentage of state tax shared with municipalities or counties.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

The bill does not grant a citizen, whose personal identifying information was stolen and who was negatively affected by a violation of this part, a cause of action against the culprit.

The Attorney General suggests that some of the language may need to be defined, such as registered owner and registration. Additionally, the Attorney General voiced concerns regarding the difficulty of enforcement of this bill for violators located in foreign countries.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE & COMBINED BILL CHANGES